ИНСТРУКЦИЯ
по организации парольной защиты при работе с информацией, содержащей данные ограниченного распространения, на автоматизированных рабочих станциях сотрудников ГБОУ СО «Гимназия № 1 (Базовая школа РАН)»

1. Общие положения

1.1. Настоящая Инструкция предназначена для использования в работе сотрудниками ГБОУ СО «Гимназия № 1 (Базовая школа РАН)», и определяет порядок обеспечения защиты локальных ресурсов отдельных рабочих станций автоматизированных рабочих мест (далее по тексту настоящей Инструкции – АРМ), использующих подсистемы парольной защиты от несанкционированного доступа (далее по тексту настоящей Инструкции – НСД) в информационных системах (далее – ИС).

1.2. Парольная защита при работе на объекте информатизации осуществляется с целью предотвращения НСД к информации, содержащей данные ограниченного распространения.

1.3. Парольная защита объекта информатизации является составной частью подсистемы управления доступом общей системы защиты от НСД.

К основным видам (категориям) паролей относятся:

- пароли доступа к локальным ресурсам отдельного компьютера (АРМ); пароли доступа к ресурсам АРМ;
- пароли доступа к прикладным программам, обеспечивающим доступ к конфиденциальной информации;
- пароли доступа средств защиты от НСД;
- пароли систем доступа, встроенные в используемые операционные системы.

2. Требования к организации парольной защиты объекта информатизации

2.1. Личный пароль доступа к информационной системе выдается пользователю организации администратором информационной безопасностиорганизации-оператора ИС.

2.2. Лица, использующие парольную защиту, обязаны:

- знать и строго выполнять требования настоящей Инструкции и других документов, регламентирующих использование парольной защиты;
- своевременно сообщать администратору информационной безопасности министерства обо всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями;
- располагать в помещении экран видеомонитора во время работы так, чтобы исключить возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами;
- обеспечивать запирание помещения на ключ при выходе всех работников из помещения, в котором осуществляется работа с информационными системами;
- поддерживать постоянную работу (не отключать (блокировать) средства защиты информации;
- передавать в случае прекращения трудовых отношений Ответственному за организацию обработки персональных данных в ИС все имеющиеся в пользовании материальные носители информации, содержащие информацию ограниченного доступа.

2.3. При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах (на корпусе монитора, на обратной стороне клавиатуры и т.д.);
- хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги, а также в электронном виде на магнитных, оптических и электронных носителях

информации;
- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД;
- создавать и хранить документы, содержащие информацию ограниченного доступа, в папках, предназначенных для обмена открытыми документами;
- работать с информацией ограниченного доступа в общественных местах и на рабочих станциях, не оборудованных средствами защиты информации;
- осуществлять обработку информации на автоматизированном рабочем месте в присутствии лиц, не допущенных к данной информации;
- оставлять без личного контроля съемные и другие носители информации (в т. ч. и установленные на автоматизированном рабочем месте), распечатки, содержащие информацию ограниченного доступа;
- записывать на устройства, предназначенные для хранения информации ограниченного доступа, посторонние данные;
- использовать информацию ограниченного доступа в личных целях, в т. ч. в целях получения выгоды;
- выносить за пределы контролируемой зоны организации материальные носители с информацией ограниченного доступа;
- оставлять без личного контроля включенное автоматизированное рабочее место без активированной блокировки

2.4. Руководители структурных подразделений организации несут персональную ответственность за организацию в своем подразделении работы по безусловному выполнению требований настоящей Инструкции и других документов, регламентирующих использование парольной защиты.

3. Порядок применения парольной защиты

3.1. Защита с применением паролей технических средств и программных продуктов осуществляется в соответствии с эксплуатационной документацией на этитехнические средства и программные продукты.

3.2. Полная плановая смена паролей на АРМ проводится регулярно, не реже одного раза в год.

3.3. Внеплановая смена (удаление) личного пароля любого пользователя должна производиться в следующих случаях:
- по окончании срока действия пароля;
- в случае увольнения, перехода на другую работу сотрудника организации, являвшегося пользователем АРМ (после окончания последнего сеанса работыданного пользователя с системой);
- при обнаружении факта успешной попытки НСД к ИС;
- при обнаружении факта компрометации базы данных (электронный или бумажный носитель, содержащей пароли пользователей).

3.4. Срок действия пароля в случае производственной необходимости определяется администратором информационной безопасности. Пароли для ИС хранятся в электронном виде у ответственного сотрудника оператора ИС.

3.5. Для предотвращения доступа к информации, данным ограниченного распространения, находящейся в ИС, минуя ввод пароля, пользователь по окончании сеанса работы или во время перерыва в работе обязан осуществить выход из ИС либопроизвести выключение ПЭВМ.

3.6. Пароли, используемые для локального доступа к программно-аппаратным средствам и доступа к ресурсам ИС вводятся пользователем с клавиатуры.

3.7. Информация о компрометации действующих паролей является чрезвычайным происшествием, доводится пользователем организации донепосредственного руководителя.

3.8. Под компрометацией понимается хищение, утрата действующих паролей, передача или сообщение их лицам, не имеющим на то право, несанкционированный доступ к данным пользователя, защищаемым паролем, другие действия ответственного исполнителя, приведшие к получению его пароля лицами, не имеющими на то право.

3.9. Скомпрометированные пароли выводятся из действия незамедлительно.
3.10. По каждому случаю, связанному с компрометацией действующих паролей, руководство организации организует и проводит в установленном порядкеслужебное расследование.

По результатам служебного расследования к лицам, допустившим разглашение паролей, могут быть применены меры дисциплинарного воздействия и иные меры, предусмотренные действующим законодательством.

4. Правила обращения со съемными носителями

Сотрудники организации используют съемные носители информации только в случаях, когда это необходимо для выполнения трудовых (служебных) обязанностей. При использовании съемных носителей сотрудники организации обязаны:

- использовать съемные носители исключительно для выполнения трудовых обязанностей и не использовать в личных целях;
- обеспечивать физическую безопасность съемных носителей;
- обеспечивать проверку отсутствия вредоносного программного обеспеченияна съемных носителях;
- извещать Ответственного за организацию обработки персональных данных в ИС о фактах утери съемных носителей, содержавших персональные данные работников и (или) обучающихся;
- не передавать съемные носители третьим лицам при отсутствии в этом производственной необходимости;
- не оставлять съемные носители без присмотра.

5. Использование электронной почты и ресурсов сети Интернет

При использовании электронной почты сотрудникам организации запрещается:

- пересылать информацию ограниченного доступа с использованием общедоступных почтовых сервисов (Яндекс, Рамблер, Mail.ru, Google и другие);
- открывать вложения подозрительных электронных сообщений: сообщений от незнакомых отправителей; сообщений, содержащих исполняемые файлы (EXE, COM, BAT); сообщений рекламного, развлекательного, оскорбительного характера; переходить по ссылкам на сайты из подозрительных электронных сообщений, в том числе сообщений, содержащих приглашения «открыть», «запустить», «посетить», «нажать», «перейти»;
- отправлять электронные письма от имени других сотрудников организации, если иное не определено их служебными обязанностями;
- предпринимать попытки несанкционированного доступа к почтовым ящикам других сотрудников организации.

При использовании ресурсов сети Интернет сотрудникам организациизапрещается:

- использовать для обмена информацией ограниченного доступа сайты представляющие услуги хранения и обмена информацией;
- размещать, публиковать информацию ограниченного доступа на общедоступных ресурсах;
- загружать из сети Интернет программное обеспечение и устанавливать его на автоматизированные рабочие места.

6. Порядок действий в случае возникновения нештатных ситуаций

При возникновении нештатных ситуаций, связанных с использованием информационной системы, а также в случаях:

- подозрения на компрометацию (утерю, разглашение, несанкционированное копирование или использование) личных паролей;
- подозрения на наличие вредоносных программ (нетипичная работа программ, появление

графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.);

- обнаружения фактов совершения в отсутствие пользователя попыток несанкционированного доступа к техническим средствам и носителям информации (следов вскрытия, измененного состава подключенных устройств, кабелей, в том числе отводов кабелей);
- невозможности запуска средств защиты информации или при ошибках в процессе их выполнения;
- несанкционированных изменений в конфигурации программного обеспечения;отклонений в нормальной работе программного обеспечения, затрудняющих
- эксплуатацию автоматизированного рабочего места;
- обнаружения ошибок в программном обеспечении, сотрудник организации обязан обратиться с описанием проблемы к ответственному за обеспечение защитыинформации лицу или ответственному за эксплуатацию ИС.

7. Ответственность сотрудников организации

Сотрудники организации несут персональную ответственность за надлежащееисполнение своих обязанностей, а также сохранность технических средств автоматизированного рабочего места, съемных носителей информации, электронных идентификаторов и целостность установленного программного обеспечения. Пользователь, виновный в нарушениях, несет ответственность, предусмотренную действующим законодательством Российской Федерации.

ЭП

O="ГБОУ СО ""
Гимназия №1
(Базовая школа
РАН)""",
CN=Загребова Л.Е.,
E=gymnasia1@mail.ru
00d52bb22ea5ebd191
2023.02.01
09:26:24+04'00'